

**IN THE CLAIMS:**

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (previously presented) A method comprising the steps of:  
disabling a data integrity function of a first data packet, said data integrity function configured for determining whether data within said first data packet is valid;  
calculating data integrity information for each of a plurality of independent data segments to be transmitted within said data packet; and  
transmitting said plurality of independent data segments and said data integrity information within said first data packet.
2. (original) The method as in claim 1 wherein said data integrity information is a checksum.
3. (original) The method as in claim 1 wherein said data integrity function is a checksum function.
4. (original) The method as in claim 1 wherein said first data packet is a User Datagram Protocol ("UDP") packet.
5. (original) The method as in claim 1 wherein said independent data segments are GSM-AMR audio frames.

6. (original) The method as in claim 4 wherein disabling said data integrity function of said first data packet comprises setting a checksum of said first data packet to zero.

7. (Currently Amended) The method as in claim 1 further comprising:  
receiving said first data packet at a client; ~~and~~  
determining whether any of said independent data segments are corrupt based on said data integrity information; and  
discarding any independent data segments which are corrupt.

8. (original) The method as in claim 7 wherein determining whether any of said independent data segments are corrupt further comprises  
recalculating said data integrity information for each of said plurality of independent data segments; and  
comparing said recalculated data integrity information with said transmitted data integrity information to determine whether any of said independent data segments are corrupt.

9. (Currently Amended) An apparatus comprising:  
a data integrity calculation module for calculating data integrity information for a plurality of independent data segments;  
a packet generation module for encapsulating said plurality of independent data segments and associated data integrity information within a data packet and disabling a data integrity function of said data packet; and

a transmission module for transmitting said data packet over a network to a destination.

10. (original) The apparatus as in claim 9 wherein said data integrity information is a checksum.

11. (original) The apparatus as in claim 9 wherein said data integrity function is a checksum function.

12. (original) The apparatus as in claim 9 wherein said data packet is a User Datagram Protocol ("UDP") packet.

13. (original) The apparatus as in claim 9 wherein said data segments are GSM-AMR audio frames.

14. (original) The method as in claim 12 wherein disabling said data integrity function of said data packet comprises setting a checksum of said first data packet to zero.

15. (previously presented) A method comprising:

providing a UDP datagram, the UDP datagram having a header and a payload, the payload comprised of a plurality of independent data segments, the header comprising a source port field, a destination port field, a length field, and a datagram checksum;

setting the datagram checksum to zero;

adding a checksum to each independent data segment in the payload;  
and  
sending the modified datagram through to a destination port.

16. (Cancelled)

17. (original) A machine-readable medium having program code stored thereon which, when executed by a machine, cause said machine to perform the operations of:

disabling a data integrity function of a first data packet, said data integrity function capable of determining whether data within said first data packet is valid;

calculating data integrity information for each of a plurality of independent data segments to be transmitted within said data packet; and

transmitting said plurality of independent data segments and said data integrity information within said first data packet.

18. (original)The machine-readable medium as in claim 17 wherein said data integrity information is a checksum.

19. (original)The machine-readable medium as in claim 17 wherein said data integrity function is a checksum function.

20. (original)The machine-readable medium as in claim 17 wherein said first data packet is a User Datagram Protocol ("UDP") packet.

21.(original)The machine-readable medium as in claim 17 wherein said independent data segments are GSM-AMR audio frames.

22. (original)The machine-readable medium as in claim 20 wherein disabling said data integrity function of said first data packet comprises setting a checksum of said first data packet to zero.

23. (Currently Amended) The machine-readable medium as in claim 17 including program code which causes said machine to perform the additional operations of:

receiving said first data packet at a client; and

determining whether any of said independent data segments are corrupt based on said data integrity information; and

discarding any independent data segments which are corrupt.

24. (original) The machine-readable medium as in claim 23 wherein determining whether any of said independent data segments are corrupt further comprises:

recalculating said data integrity information for each of said plurality of independent data segments; and

comparing said recalculated data integrity information with said transmitted data integrity information to determine whether any of said independent data segments are corrupt.

## **COMMENTS**

The enclosed is responsive to the Examiner's Final Office Action mailed on August 16, 2004 and is being filed pursuant to a Request for Continued Examination (RCE) as provided under 37 CFR 1.114. At the time the Examiner mailed the Office Action claims 1-15 and 17-24 were pending. By way of the present response the Applicant has: 1) added no claims; 2) cancelled no claims; 3) and amended claims 7, 9 and 23. As such, claims 1-15 and 17-24 are now pending. The Applicant respectfully requests reconsideration of the present application and the allowance of all pending claims.

### **Claim Rejections**

#### **35 U.S.C. §103(a) Rejections**

The Examiner rejected claims 1-6, 9-15, 17, 18-22 under 35 U.S.C. 103(a) as being unpatentable over Jonsson, U.S. Patent 6,609,224 (hereinafter "Jonsson") in view of Kato, U.S. Patent 5,844,918 (hereinafter "Kato").

Examiner asserts that, "calculating data integrity information for each of a plurality of independent data segments to be transmitted within said data packet" of claim 1 is disclosed in Kato. Examiner cites to col. 5, lines 28-35 in support.

Applicant respectfully submits that Kato does not disclose this limitation of claim 1.

Claim 1 states:

1. (previously presented) A method comprising the steps of:

disabling a data integrity function of a first data packet, said data integrity function configured for determining whether data within said first data packet is valid;  
calculating data integrity information for each of a plurality of independent data segments to be transmitted within said data packet; and  
transmitting said plurality of independent data segments and said data integrity information within said first data packet.  
(emphasis added)

By contrast, Kato states:

a division step of dividing an error correcting code which includes data complete with a parity code, into smaller data segments;  
an error detecting code addition step of appending an error detecting code to each of the data segments divided in the division step;  
a transmission step of sending the data segments complete with the error detecting code on a packet-by-packet basis; (Col. 5, lines 28-35)

Thus, Kato fails to disclose calculating data integrity information for each of a plurality of independent data segments to be transmitted with said data packet.

There is no mention in Kato of the data segments being independent. Kato merely discloses dividing an error correcting code into smaller data segments which are inherently dependent on one another (i.e., because they include information related to the initial error correcting code).

Further, Kato fails to disclose the calculating data integrity information for each independent data segment. Kato merely discloses the appending an error detecting code to each data segment.

Examiner specifically states that Jonsson does not teach this limitation of claim 1. "Jonsson does not explicitly teach calculating data integrity information for [independent] data segments to be transmitted within the data packet." Office action, pg.4. Therefore the combination of Kato and Jonsson fail to make claim 1 obvious under 35 U.S.C. §103(a).

Independent claims 9, 15 and 17 also contain this limitation of claim 1, therefore the combination of Kato and Jonsson also fail to make these claims obvious under 35 U.S.C. §103(a).

Dependent claims 2-8, 10-14 and 18-24 all depend upon and include the limitations of independent claims 1, 9, 15 and 17. Therefore the combination of Kato and Jonsson also fail to make these claims obvious under 35 U.S.C. §103(a).

In light of the comments above, the Applicant respectfully requests the allowance of all pending claims.



**CONCLUSION**

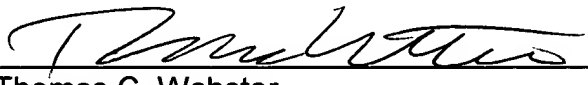
Applicant respectfully submits that all rejections have been overcome and that all pending claims are in condition for allowance.

If there are any additional charges, please charge them to our Deposit Account Number 02-2666. If a telephone conference would facilitate the prosecution of this application, the Examiner is invited to contact Thomas C. Webster at (408) 720-8300.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 12/16/04

  
Thomas C. Webster  
Reg. No. 46,154

12400 Wilshire Blvd.  
Seventh Floor  
Los Angeles, CA 90025-1030  
(408) 720-8300